

# Origami rings

Joe Buhler <sup>\*</sup>    Steve Butler<sup>†</sup>    Warwick de Launey<sup>‡</sup>    Ron Graham <sup>§</sup>

## Abstract

Motivated by a question in origami, we consider sets of points in the complex plane constructed in the following way. Let  $L_\alpha(p)$  be the line in the complex plane through  $p$  with angle  $\alpha$  (with respect to the real axis). Given a fixed collection  $U$  of angles, let  $R(U)$  be the points that can be obtained by starting with 0 and 1, and then recursively adding intersection points of the form  $L_\alpha(p) \cap L_\beta(q)$ , where  $p, q$  have been constructed already, and  $\alpha, \beta$  are distinct angles in  $U$ .

Our main result is that if  $U$  is a group with at least three elements, then  $R(U)$  is a subring of the complex plane, i.e., it is closed under complex addition and multiplication. This enables us to answer a specific question about origami folds: if  $n \geq 3$  and the allowable angles are the  $n$  equally spaced angles  $k\pi/n$ ,  $0 \leq k < n$ , then  $R(U)$  is the ring  $\mathbf{Z}[\zeta_n]$  if  $n$  is prime, and the ring  $\mathbf{Z}[1/n, \zeta_n]$  if  $n$  is not prime, where  $\zeta_n := \exp(2\pi i/n)$  is a primitive  $n$ -th root of unity.

**AMS 2010 subject classification:** 11R04; 11R18; 00A08

**Keywords:** origami; rings; sine-quotients; monomials

## 1 Introduction

Origami constructions start with a flat sheet of paper and, through a series of folds, arrive at a three-dimensional figure. Some of the folds produce pleats, whereas others produce needed reference points. More information about the techniques of origami design with some amazing origami figures can be found in Lang [5], and some mathematical aspects of origami can be found in [1] and [2].

---

<sup>\*</sup>Center for Communications Research, La Jolla, CA 92121 ([buhler@ccrwest.org](mailto:buhler@ccrwest.org))

<sup>†</sup>Department of Mathematics, UCLA, Los Angeles, CA 90095 ([butler@math.ucla.edu](mailto:butler@math.ucla.edu)).

This work was done with support of an NSF Mathematical Sciences Postdoctoral Fellowship.

<sup>‡</sup>Center for Communications Research, La Jolla, CA 92121 ([warwickdelauney2010@earthlink.net](mailto:warwickdelauney2010@earthlink.net))

<sup>§</sup>Department of Computer Science and Engineering, University of California, San Diego, La Jolla, CA 92093 ([graham@ucsd.edu](mailto:graham@ucsd.edu)).

The sets of reference points that can be constructed under various assumptions has been studied for theoretical reasons — e.g., solving quartic equations [4, pp. 285–291] — or for more practical reasons — e.g., approximating desired reference points [6].

We will consider an idealized form of paper folding and determine the set of reference points that can be constructed by folds in a fixed set of directions (i.e., angles), where new points are found as intersections of folds through points that have already been constructed. As a basic example, the set of all points constructed from the points 0 and 1 with angles chosen from  $\{0, \pi/3, 2\pi/3\}$  is the hexagonal lattice  $\mathbf{Z}[\zeta_3]$  in the complex plane  $\mathbf{C}$  (see Figure 1), as the reader may enjoy verifying.

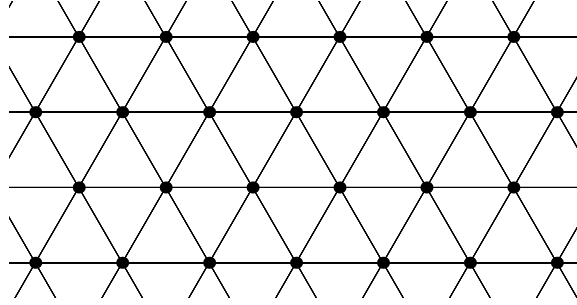


Figure 1: The hexagonal lattice  $\mathbf{Z}[\zeta_3]$ .

For  $u \neq 0$ , the line through 0 and  $u$  determines an angle with the real axis. Since nonzero real multiples of  $u$  determine the same angle as  $u$ , without loss of generality we may assume  $u$  has absolute value 1, i.e., that  $u$  is on the unit circle  $\mathbf{T}$  in the complex plane. In addition, since  $u$  and  $-u$  also determine the same angle, we choose to think of angles as elements of the quotient group  $\mathbf{T}/\{\pm 1\}$  of the unit circle by its subgroup  $\{\pm 1\}$  of order 2. We will abuse notation in the usual way and also refer to elements of  $\mathbf{T}$  as angles. Also, note that the  $1 \in \mathbf{T}/\{\pm 1\}$  corresponds to a horizontal line (parallel to the real axis). The reader could alternatively choose to identify this group with the group  $\mathbf{R}/\pi\mathbf{Z}$  of real numbers in  $[0, \pi)$  under addition modulo  $\pi$ , where  $\theta$  corresponds to  $e^{i\theta}$  in the formulas to follow. In this setting, the horizontal line has angle 0.

To simplify and symmetrize our constructions, we will always assume our collection  $U$  of angles is a group, i.e., that it is a subgroup of  $\mathbf{T}/\pm 1$ . If  $U$  is finite, then it is cyclic; let  $U_n$  denote the group of angles that is cyclic of order  $n$  generated by  $e^{i\pi/n}$ . Thus the collection  $\{0, \pi/3, 2\pi/3\}$  mentioned above corresponds to  $U_3$ .

If  $p$  is a point in the plane and  $u$  is an angle then

$$L_u(p) := \{p + ru : r \in \mathbf{R}\}$$

is the line through  $p$  with angle  $u$ . We define the intersection

$$I_{u,v}(p, q) := L_u(p) \cap L_v(q)$$

to be the unique point on the intersection of the lines  $L_u(p)$  and  $L_v(q)$ , when  $u$  and  $v$  are distinct angles. Note that the slopes of the two lines are distinct, so the intersection exists and is unique.

In general, given an initial (or seed) set  $S$  lying in a set  $X$  on which a collection of binary operators acts, it is natural to recursively define  $S_0 = S$ , and  $S_{n+1}$  to be the set obtained by applying all operators to (pairs of) elements of  $S_n$ . The union of the  $S_n$  is the set generated by the seed points  $S$  by iterating the action of the operators, this can also be defined as the smallest subset of  $X$  that contains  $S$  and is closed under the given set of operators.

We are interested in the case where the initial set  $S$  consists of the two points 0 and 1, and the operators are the set of  $I_{u,v}$  where  $u$  and  $v$  range over distinct angles in  $U$ . We let  $R(U)$  denote the smallest subset of the complex plane that contains  $\{0, 1\}$  and is closed in the sense that if  $p$  and  $q$  are in the set, and  $u$  and  $v$  are distinct elements of  $U$ , then  $I_{u,v}(p, q)$  is also in the set.

Our main result is the (perhaps slightly surprising) fact that  $R(U)$  is a subring of  $\mathbf{C}$  if  $U$  has at least 3 elements. Moreover, the elements of  $R(U)$  can be described explicitly.

**Theorem 1.** *With the above notation, if  $U$  has at least 3 elements then  $R(U)$  is a subring of  $\mathbf{C}$ , consisting of all integral linear combinations of “monomials,” which are arbitrary finite products of complex numbers of the form*

$$\frac{1 - u^2}{1 - v^2}$$

where  $u$  and  $v$  are in  $U$ . (Note that  $u^2 \in \mathbf{T}$  is independent of the choice of representative of the class of  $u \in \mathbf{T}/\{\pm 1\}$ .)

This enables us to give a precise description of the ring when  $U$  is finite.

**Theorem 2.** *Let  $n \geq 3$ . If  $n$  is prime, then  $R(U_n) = \mathbf{Z}[\zeta_n]$  is the cyclotomic integer ring. If  $n$  is not a prime then  $R(U_n) = \mathbf{Z}[1/n, \zeta_n]$  is the cyclotomic integer ring localized at (the primes dividing)  $n$ .*

This generalizes the  $n = 3$  result mentioned above, but, as we will explain later, that case is an outlier: for  $n > 3$ ,  $R(U_n)$  is a dense subset of the complex plane.

## 2 Plane intersections

The goal of this section is to describe basic facts about the intersection point  $I_{u,v}(p, q)$ , both from algebraic and geometric perspectives.

Let  $u, v$  be distinct angles, and consider the lines  $L_u(p)$  and  $L_v(q)$ . The intersection of these lines is the point  $I_{u,v}(p, q)$  that is the unique solution to

$$z = p + ru = q + sv,$$

for  $r, s$  real numbers. Since  $s$  is real then the imaginary part of  $s = v^{-1}(p - q + ru)$  must equal zero. This gives an equation that can be solved for  $r$ , yielding

$$r = \frac{\operatorname{Im}((q - p)/v)}{\operatorname{Im}(u/v)}.$$

It is convenient to introduce the notation

$$[x, y] = xy^* - x^*y = 2i |y|^2 \operatorname{Im}(x/y)$$

where  $x^*$  denotes the complex conjugate of  $x$ , and  $|y|^2 = y^*y$ . Note that  $[\cdot, \cdot]$  is additive, real-linear, and antisymmetric. We can now rewrite the equation for  $r$  in the form

$$r = \frac{[q - p, v]}{[u, v]}.$$

This gives

$$I_{u,v}(p, q) = p + \frac{[q - p, v]}{[u, v]} u = \frac{[u, v]p + [q, v]u - [p, v]u}{[u, v]}.$$

Substituting the definition and doing some algebraic juggling leads to a fundamental formula:

$$I_{u,v}(p, q) = \frac{up^*v - u^*pv - vq^*u + v^*qu}{[u, v]} = \frac{[u, p]}{[u, v]}v + \frac{[v, q]}{[v, u]}u. \quad (1)$$

A number of basic facts follow from this formula.

**Proposition 3.** *Let  $p, q$  be points in the plane, and  $u, v$  be pairwise distinct angles.*

- (Symmetry)  $I_{u,v}(p, q) = I_{v,u}(q, p)$
- (Reduction)  $I_{u,v}(p, q) = I_{u,v}(p, 0) + I_{v,u}(q, 0)$
- (Projection)  $I_{u,v}(p, 0)$  is a projection of  $p$  onto the line  $\{rv : r \in \mathbf{R}\}$  in the direction  $u$
- (Linearity)  $I_{u,v}(p + q, 0) = I_{u,v}(p, 0) + I_{u,v}(q, 0)$  and, for real  $r$ ,  $I_{u,v}(rp, 0) = r I_{u,v}(p, 0)$
- (Convexity)  $I_{u,v}(p, q)$  has the form  $Ap + Bq$  where  $A$  and  $B$  are real-linear maps of the complex plane that satisfy  $A + B = 1_{\mathbf{C}}$ , where  $1_{\mathbf{C}}$  is the identity map on the plane
- (Rotation) For  $w \in \mathbf{T}$ ,  $wI_{u,v}(p, q) = I_{wu, wv}(wp, wq)$ .

**Remarks.** 1. The projection of  $p$ , onto a line  $L$  in the direction  $u$ , is the point of the form  $p + ru$  that lies on the line  $L$ .

2. Real-linear maps of the plane can be written in two useful forms: as maps taking  $p$  to  $p' = ap + bp^*$  for complex constants  $a, b$ , or as maps taking  $p = x + iy$  to  $p' = x' + iy'$  written in terms of two by two matrices:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

where  $a, b, c, d$  are real.

3. The use of the term “Convexity” is merely by vague analogy with the operation  $tx + (1-t)y$  taking elements  $x, y$  of a real vector space to a convex combination on the line between them, where  $t \in [0, 1]$ .

The verifications of the facts in the proposition from the identity (1) are straightforward algebraic exercises which we leave to the reader. However, these facts can also be verified geometrically, as we now briefly sketch.

Symmetry follows from the fact that both sides of the equation solve the same intersection problem. Reduction is the Law of Parallelograms (see Figure 2a) and Symmetry. Projection follows from another straightforward diagram. Linearity follows from Projection and the fact that projections are linear (see Figure 2b). Convexity follows from Reduction, the fact that each term in the Reduction formula is a projection, and the fact that if  $p = q$  then  $I_{u,v}(p, q) = p$ . (Note that the linear maps  $A, B$  have rank 1, since they are projections.) Rotation expresses the fact that if the points and angles of an intersection problem are all rotated by an angle  $w$  then the result is rotated by  $w$ .

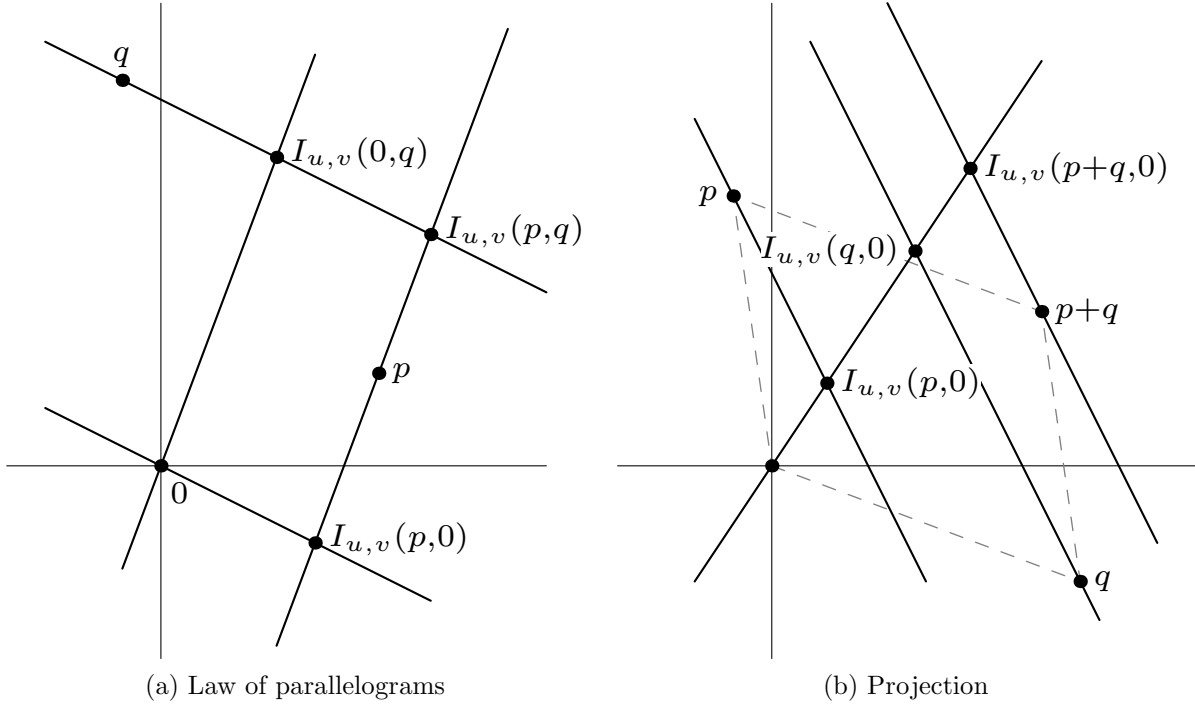


Figure 2: Properties of  $I_{u,v}(p, q)$

### 3 Closure under addition and multiplication

Recall for a fixed group  $U$  of angles,  $R(U)$  denotes the smallest set of complex numbers that contains 0 and 1 and has the property that if  $u, v$  are distinct elements of  $U$ , and  $p, q$  are

elements of  $R(U)$ , then  $I_{u,v}(p, q)$  is in  $R(U)$ . Theorem 1 asserts that if  $U$  has size at least three then  $R(U)$  is a subring of  $\mathbf{C}$ , i.e., that  $R(U)$  is closed under addition and multiplication.

This will be proved in a series of lemmas.

**Lemma 4.**  *$R(U)$  is closed under addition.*

*Proof.* First, note that 2 is in  $R(U)$ . Indeed, if  $u, v$  are distinct nonzero angles in  $U$  then construct the following points:

$$p_1 = I_{u,v}(0, 1), \quad p_2 = I_{u,1}(1, p_1), \quad p_3 = I_{1,v}(0, p_2).$$

Some slightly involved algebra shows that  $p_3 = 2$ , but this is also geometrically obvious as a quick glance at Figure 3 shows.

Moreover, if  $p$  is in  $R(U)$  then so is  $p + 1$ . Indeed, apply the steps that were used to construct  $p$  starting from 0 and 1, but instead starting at the points 1 and 2; the result is  $p + 1$ . Similarly, if  $p$  and  $q$  are in  $R(U)$  then so is their sum: repeating the steps used to construct  $q$ , starting from  $p$  and  $p + 1$ , gives  $p + q$ .  $\square$

**Lemma 5.**  *$R(U)$  is closed under taking additive inverses.*

*Proof.* First, note that  $-1$  is in  $R(U)$ . Indeed, if  $p_1 = I_{u,v}(0, 1)$  as above, and  $p'_2 = I_{v,1}(0, p_1)$  then it is easy to verify geometrically or algebraically that  $-1 = I_{1,u}(0, p'_2)$  (see Figure 3). If  $p$  is in  $R(U)$  then  $-p$  can be constructed by applying the steps used to construct  $p$ , except that we start at 0 and  $-1$ .  $\square$

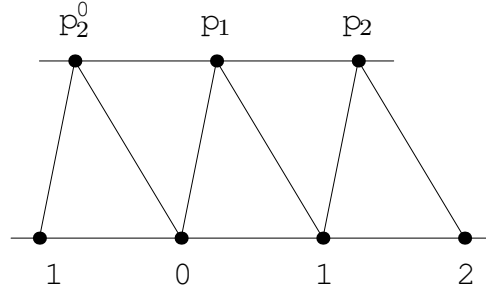


Figure 3:  $-1$  and  $2$ .

A point  $p$  in  $R(U)$  is said to be a *monomial* (or, if the emphasis is needed, a  $U$ -monomial) if it can be produced starting at 1 using only intersections of the form  $I_{u,v}(p, 0)$ , i.e., intersections in which the second line is required to go through the origin. Thus a monomial lies in a sequence of the form

$$p_1 = I_{u_1,v_1}(1, 0), \quad p_2 = I_{u_2,v_2}(p_1, 0), \quad p_3 = I_{u_3,v_3}(p_2, 0), \quad \dots$$

If  $p = p_n = I_{u_n,v_n}(p_{n-1}, 0)$  occurs at the  $n$ -th step, then  $p$  is said to be a monomial of length at most  $n$ . In terms of the linear operators  $A$  in the Convexity property, this could be written

$$p = A_n A_{n-1} \cdots A_2 A_1 1$$

where  $A_i$  is the linear operator occurring in the  $i$ -th step.

A monomial  $p = I_{u,v}(1, 0)$  of length 1 is said to be an *elementary* monomial.

**Lemma 6.**  *$R(U)$  is the set of (finite) integer linear combinations of monomials.*

*Proof.* Since  $R(U)$  is closed under addition and contains  $-1$  it is obvious that  $R(U)$  contains all linear combinations of monomials with coefficients in  $\mathbf{Z}$ .

To prove that  $R(U)$  consists exactly of those elements, use induction on the length of the constructions. Specifically, we prove that elements of  $R(U)$  constructed with at most  $n$  intersection operations are linear combinations of monomials of length at most  $n$ . The base cases are obvious. If  $p$  and  $q$  can be constructed with at most  $n$  operations, then consider a point  $z = I_{u,v}(p, q)$  that can be constructed in  $n+1$  operations. By the induction assumption,  $p$  and  $q$  are sums of monomials of length at most  $n$ . By Reduction and Linearity  $z$  is a linear combination of terms of the form  $I_{u,v}(m, 0)$  where  $m$  is a monomial of length at most  $n$ . It follows that  $z$  is a linear combination of monomials of length at most  $n+1$ .  $\square$

**Lemma 7.** *The product of two monomials is a monomial. Any monomial is a product of elementary monomials. The set  $R(U)$  is closed under multiplication.*

*Proof.* For the first two statements, the key idea is the Rotation property (or, that the set of operators is normalized by rotations). The identity

$$I_{u,v}(1, 0)I_{u',v'}(1, 0) = rv I_{u',v'}(1, 0) = r I_{vu',vv'}(v, 0) = I_{vu',vv'}(rv, 0) = I_{vu',vv'}(I_{u,v}(1, 0), 0)$$

(where  $r = [u, 1]/[u, v] \in \mathbf{R}$ ) shows that the product of two elementary monomials is a monomial of length 2, and conversely. Everything else is induction.

For instance, assume that the product of two monomials is a monomial when the sum of the lengths is at most  $n$ . Let  $m'$  be a monomial of length at most  $a$ , and  $m$  be a monomial of length at most  $b$  where  $a + b = n$ . Then consider a product of monomials of length  $a + 1$  and  $b$ :

$$m I_{u,v}(m', 0).$$

Write  $m = tw$  where  $t$  is real and  $w$  is on the unit circle. Use Rotation and Linearity to get

$$m I_{u,v}(m', 0) = tw I_{u,v}(m', 0) = I_{wu,wv}(twm', 0) = I_{wu,wv}(mm', 0).$$

Since  $mm'$  is a monomial by the induction assumption, it follows that the right-hand side is a monomial. A similar induction argument proves the converse.

The last statement of the lemma follows immediately from the first statement, using the preceding lemma.  $\square$

This finishes the proof that  $R(U)$  is a subring of the complex numbers.

**Remarks.** 1. The fact that our allowable angles  $U$  formed a group was only used in the last lemma, where we needed closure under multiplication.

2. Many of the facts can be proved under weaker hypothesis, and these results might be useful in other contexts. For instance, if we consider more general operators  $Ap+Bq$ , as in the Convexity property, applied recursively to a set of seed points, then closure under addition is implied by (and therefore equivalent to) the fact that 2 can be constructed. In similar more general contexts, the property of being closed under multiplication comes down to the set of operators being normalized by rotations (multiplying by elements of  $\mathbf{T}$ ).

## 4 Ring generators

Throughout this section let  $U$  be a group of angles with 3 or more elements, and let  $U_n$  denote the cyclic group of order  $n$  of angles generated by  $e^{i\pi/n}$ , for  $n \geq 3$ .

From the proof of multiplicative closure, monomials have the form

$$\frac{[u_1, 1]}{[u_1, v_1]} \frac{[u_2, u_1]}{[u_2, v_2]} \cdots \frac{[u_n, u_{n-1}]}{[u_n, v_n]} v_n.$$

If  $u = e^{i\pi a}$ ,  $v = e^{i\pi b}$ , and  $w = e^{i\pi c}$  then

$$\frac{[u, w]}{[u, v]} = \frac{\sin(\pi(a - c))}{\sin(\pi(a - b))}$$

and we sometimes refer to these as “sine-quotients.” Thus we can say that a monomial is a product of sine-quotients by an element of  $U$ .

The proof of multiplicative closure also showed that monomials are products of elementary monomials. Note that an elementary monomial can be written, using  $v = 1/v^*$ , as

$$I_{u,v}(1, 0) = \frac{[u, 1]}{[u, v]} v = \frac{u - u^*}{u(v^*)^2 - u^*} = \frac{1 - u^2}{1 - (u/v)^2}.$$

As  $u$  and  $v$  range over all angles, this quotient ranges over all quotients of the form  $(1 - u)/(1 - v)$  where  $u$  and  $v$  are elements of the group  $V := \{u^2 : u \in U\} \subset \mathbf{T}$  obtained by taking representatives of elements of  $U$ , in the circle group, and squaring. (Note that  $V$  is isomorphic to  $U$ ; indeed, the squaring map induces an isomorphism  $\mathbf{T}/\{\pm 1\} \simeq \mathbf{T}$ , and  $V$  is the image of  $U$  under this map.)

Combining all of these facts gives a proof of the basic assertion made about  $R(U)$  in the introduction.

**Theorem 8.** *Let  $U$  be a group of angles with at least three elements, and let  $V \subset \mathbf{T}$  be the group of squares described above. Then  $R(U)$  is the subring of  $\mathbf{C}$  consisting of linear combinations of monomials, with coefficients in  $\mathbf{Z}$ , where monomials are products of elements of the form*

$$\frac{1 - u}{1 - v}$$

*for  $u$  and  $v$  in  $V$ ,  $v \neq 1$ .*



Recall that the cyclotomic field  $\mathbf{Q}(\zeta_n)$  is the smallest subfield of  $\mathbf{C}$  that contains the primitive  $n$ -th root of unity  $\zeta_n := e^{2\pi i/n}$ . It is a standard fact from algebra that  $\mathbf{Q}(\zeta_n)$  is the set of rational functions in  $\zeta_n$ , over  $\mathbf{Q}$ , and that it can be described even more simply as the set of rational linear combinations of powers of  $\zeta_n$ . The group  $U_n$  is generated by (the class of)  $\zeta_{2n} = e^{i\pi/n}$ , and its group  $V_n$  of squares is generated by  $\zeta_n$ . The preceding theorem immediately implies the following corollary.

**Corollary 9.** *Every element of  $R(U_n)$  lies in the cyclotomic field  $\mathbf{Q}(\zeta_n)$ .*

**Remarks.** 1. The equality between the two formulas for  $I_{u,v}(0, 1)$

$$\frac{[u, 1]}{[u, v]} v = \frac{1 - u^2}{1 - (u/v)^2}$$

is crucial in the above analysis, but it is also curious from a field-theoretic point of view. The right hand side is obviously in  $\mathbf{Q}(\zeta_n)$ . However, the left-hand side is a product of a power of  $\zeta_{2n}$  and a sine-quotient lying in the totally real subfield of  $\mathbf{Q}(\zeta_{2n})$ .

2. For later use, we remark that if  $d$  is a divisor of  $n$  then

$$\zeta_n^{n/d} = \zeta_d.$$

The sine-quotients that arise in the above algebra are familiar (at least when  $n$  is prime) from algebraic number theory as “cyclotomic units”. To analyze the integrality properties of these quotients we need to recall some algebraic number theory.

The algebraic integers in the field  $\mathbf{Q}(\zeta_n)$  form a ring  $\mathbf{Z}[\zeta_n]$  consisting of integral linear combinations of powers of  $\zeta_n$ . The following facts can be found in many texts on algebraic number theory, such as [3], and we include brief proofs for the convenience of the reader.

**Theorem 10.** *Fix  $n > 3$ , let  $\zeta = \zeta_n$ , and assume throughout that  $a$  and  $b$  are nonzero modulo  $n$ .*

- (a) *If  $n$  is prime, then  $(1 - \zeta^a)/(1 - \zeta^b)$  is an algebraic integer.*
- (b) *If  $n$  is non-prime, then  $(1 - \zeta^a)/(1 - \zeta^b)$  has denominator dividing  $n$ .*
- (c) *If  $n$  is non-prime and  $p$  is a prime divisor of  $n$ , then some product of an element of  $\mathbf{Z}[\zeta_n]$  by a product of quotients of the form  $(1 - \zeta^a)/(1 - \zeta^b)$  is equal to  $1/p$ .*

*Proof.* If  $n$  is prime then  $b$  is relatively prime to  $n$ , and we can solve the equation  $a + rn = bs$  in integers  $r, s$ . Then

$$\frac{1 - \zeta^a}{1 - \zeta^b} = \frac{1 - \zeta^{a+rn}}{1 - \zeta^b} = \frac{1 - \zeta^{bs}}{1 - \zeta^b}$$

is obviously a polynomial in  $\zeta$  and hence an algebraic integer. This proves (a).

To prove the next two parts of the theorem we start with the identity

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \zeta^k).$$

Divide by  $X - 1$  and take the limit as  $X \rightarrow 1$  to get

$$n = \prod_{k=1}^{n-1} (1 - \zeta^k). \quad (2)$$

(We will refer to this as equation  $(2)_n$ .) It follows from  $(2)_n$  that  $1 - \zeta^k$  is a divisor of  $n$ , for all  $k$  not divisible by  $n$ , proving (b).

To prove (c), note that it suffices to consider the cases  $n = pq$  and  $n = p^2$ , where  $p$  and  $q$  are primes. Indeed, if  $n$  is non-prime then some divisor  $d$  of  $n$  has one of those forms, and we can confine ourselves to looking at quotients  $(1 - \zeta^a)/(1 - \zeta^b)$  where both  $a$  and  $b$  are multiples of  $n/d$ , which is equivalent to restricting to  $n$  of those two forms.

If  $n = pq$  then divide equation  $(2)_n$  by equations  $(2)_p$  and  $(2)_q$  to get  $1 = \prod (1 - \zeta^k)$  where  $k$  ranges over integers relatively prime to  $n$ . It follows that  $1 - \zeta$  is a unit in  $\mathbf{Z}[\zeta]$ . Dividing  $(1 - \zeta)^{p-1}$  by equation  $(2)_p$  gives

$$\frac{u}{p} = \prod_{k=1}^{p-1} \frac{1 - \zeta}{1 - \zeta^{qk}}$$

where  $u$  is a unit, and we recall that  $\zeta^q = \zeta_p$ . Thus  $1/p$  is a product of the claimed form.

If  $n = p^2$  then careful use of equations  $(2)_{p^2}$  and  $(2)_p$  shows that

$$\prod \frac{1 - \zeta^{pk}}{1 - \zeta^k} = \frac{1}{p^{p-1}}$$

where the product is over  $k$  up to  $p^2$  and relatively prime to  $p$ . Multiplying by  $p^{p-2}$  gives  $1/p$  as desired.  $\square$

Our main theorem about  $R(U_n)$  follows easily.

**Theorem 11.** *If  $n = p$  is prime, then  $R(U_n)$  is equal to  $\mathbf{Z}[\zeta_n]$ . If  $n$  is non-prime, then  $R(U_n)$  is equal to  $\mathbf{Z}[1/n, \zeta_n]$ .*

*Proof.* The ring  $R(U_n)$  contains  $-1$  and

$$\frac{1 - \zeta}{1 - \zeta^{-1}} = -\zeta$$

so it contains  $\mathbf{Z}[\zeta_n]$ . If  $n$  is prime then the first part of the preceding theorem says that elementary monomials, and hence all monomials, are in  $\mathbf{Z}[\zeta_n]$ , and it follows that every

element of  $R(U_n)$  is contained in that ring and we are done. If  $n$  is non-prime, then every element of  $R(U_n)$  is contained in  $\mathbf{Z}[1/n, \zeta_n]$ , by the second part of the preceding theorem. However, it is also easy to construct  $1/n$  by using the third part of the preceding theorem, and hence any element of that ring, so that any element of  $\mathbf{Z}[1/n, \zeta_n]$  is in  $R(U)$ , and  $R(U_n) = \mathbf{Z}[1/n, \zeta_n]$  as claimed.  $\square$

**Corollary 12.** *If  $n > 3$  then  $R(U_n)$  is dense in the complex plane.*

*Proof.* It is well-known in algebraic number theory that  $\mathbf{Z}[\zeta_n]$  is dense in the plane if  $n \geq 4$ , and the result follows easily. However, it can also be proved directly: denseness of the ring  $R(U_n)$  is equivalent to showing that 0 is a cluster point of  $R(U_n)$ , which in turn is equivalent to finding a nonzero element of  $R(U_n)$  inside the unit circle (since powers of such an element converge to 0). This is obvious for non-prime  $n$ , so we need only consider primes  $n \geq 5$ . In this case

$$\frac{1 - \zeta}{1 - \zeta^2} = \frac{1}{1 + \zeta}$$

is easily verified to be a unit lying inside the unit circle.  $\square$

## 5 Concluding remarks

Motivated by a question about origami constructions for which the folds are limited to a finite set of directions, we have been led to a general construction in which a group of angles  $U$  gives rise to a subring  $R(U)$  of the complex plane. When combined with standard results from the theory of cyclotomic fields, the ring  $R(U)$ , this gives an explicit description of  $R(U)$  in the motivating case in which  $U$  is finite.

This may not be terribly useful in real-world origami. In the case of  $U_n$ , there is the problem about how to fold the angles in the first place; in addition, although our proofs are constructive they are likely to produce tedious series of folds — in the real world, approximations with few folds would be much more valuable.

However, the mathematical ideas that arise seem to lead to interesting questions, and we mention several.

The set  $R(U)$  can be a ring even if  $U$  is only closed under multiplication and not necessarily under inversion. It is even a ring in the case  $U = \{0, \pi/4, \pi/2\}$ . Which sets of angles  $U$  give rise to sets that are closed under complex multiplication?

Which subrings of  $\mathbf{C}$  are of the form  $R(U)$  for some group  $U$  of angles?

Given a collection  $\{A_i\}$  of  $\mathbf{R}$ -linear maps on the complex plane, define  $B_i = 1_{\mathbf{C}} - A_i$ , and consider the operators

$$I_i(p, q) = A_i p + B_i q$$

on the complex plane. Given two seed points, recursively apply these operators to build the subset of the plane of all points that are constructable from the given set of operators. (By Convexity, this generalizes  $R(U)$ .) What can be said about these sets?

# Acknowledgments

We thank Erik Demaine for originally suggesting this problem to us.

# References

- [1] Roger C. Alperin, *A mathematical theory of origami constructions and numbers*, New York J. Math. 6 2000, 119–133.
- [2] Roger C. Alperin and Robert J. Lang, One-, two-, and multi-fold origami axioms. Origami<sup>4</sup>, 371–393, A K Peters, Natick, MA, 2009.
- [3] Lawrence Washington, *Introduction to Cyclotomic Fields, Second edition*, Springer-Verlag, New York, 1997, xiv+487 pp.
- [4] Erik D. Demaine and Joseph O’Rourke, *Geometric Folding Algorithms: Linkages, Origami, Polyhedra*, Cambridge University Press, 2007, xiii+472.
- [5] Robert J. Lang, *Origami Design Secrets*, AK Peters Ltd., 2003, vii+585 pp.
- [6] Robert J. Lang, REFERENCEFINDER, available online at <http://www.langorigami.com/science/reffinder/reffinder.php4>.